STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

MANAGING RISK TO THE NATIONAL INFORMATION INFRASTRUCTURE

BY

COLONEL JAMES H. THOMAS
United States Army

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

MANAGING RISK TO THE NATIONAL INFORMATION INFRASTRUCTURE

by

Colonel James H. Thomas

Dr. Douglas V. Johnson
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: James H. Thomas, COL, USA

TITLE: Managing Risk to the National Information Infrastructure

FORMAT: Strategy Research Project

DATE: 8 April 1998 PAGES:38 CLASSIFICATION: Unclassified

Now, more than ever, the survival of our information based society depends on the integrity of our National Information Infrastructure (NII). Our information systems are vulnerable to a wide spectrum of threat ranging from a dissatisfied employee to a coordinated transnational attack to gain strategic advantage.

Interconnected military, government and civilian information systems throughout our critical infrastructures, with limited self-protection features, are susceptible and attractive targets. The NII suffers attack almost constantly and we must do better at dealing with the consequences of such attacks.

The ends, ways and means of managing the consequences of malevolent intrusion into the NII are within the capabilities of the nation to implement. Our success at dealing with these assaults, thus preventing an adversary from gaining strategic advantage jeopardizing our way of life will hinge on taking action to resolve the technological, legal, and sociological impediments to information infrastructure protection.

TABLE OF CONTENTS

LIST OF TABLES

"Our response to information warfare threats to the United States may present the greatest challenge in preparing for the security environment of 2010-2020."

National Defense Panel[1]

Now, more than ever, the survival of our information based society depends on the integrity of our National Information Infrastructure (NII)[2]. The NII has become the most vulnerable point in our national security.

Cyber attacks on the NII cut to the heart of our national interests. Not only does the military depend on accurate and timely information as an enabler, but the economic engine of our nation does as well. Our information systems are vulnerable to a wide spectrum of threat ranging from a dissatisfied employee to a coordinated transnational attack to gain strategic advantage. And our vulnerability increases proportionally to our reliance on automated information systems.

National leaders have developed national security strategy resting upon information viability. Many of the ways and means to meet this end have focused on protecting the NII, with little attention paid to managing the consequences of cyber attack upon our largely unsecured and commercially operated information infrastructure.

NATIONAL INFORMATION CENTER OF GRAVITY

Our national security relies on the NII. Information technologies are increasingly critical to our continued application of national power around the globe. Early in the Clinton administration, the Undersecretary of Commerce for International Trade, Jeffrey Garten, emphasized that the NII clearly played an important part in our economic diplomacy. The United States has a $7 trillion economic engine, but most of it exists only in electronic format in the NII. In Undersecretary Garten's view, America must maintain its lead in information technology. This lead will give our country market domination resulting in a strategic advantage for encouraging open markets, opening societies and spreading our democratic ideals.[3]

In his National Security Strategy for a New Century, President Clinton calls for fully implementing measures "to ensure the future security of not only our national information infrastructures, but our nation as well."[4]

Congress has also recognized how critical protecting the NII has become and have emphasized to the Administration they view its protection as a serious matter. The National Defense Authorization Act for Fiscal Year 1997 requires the President to report to Congress on the national policy for protecting the NII against strategic attacks.

In an effort to articulate and implement the Administration's vision for the NII, the White House formed the Information Infrastructure Task Force in 1993, led by vice President Gore and consisting of high level representatives of Federal agencies that guide the development of information technologies. One of the items for action of this task force is to identify goals ensuring information security and network reliability.[5]

More recently, the President Clinton issued Executive Order 13010, 15 July 1996, directing the protection of critical infrastructures from physical and "cyber" threats.[6] This executive order resulted in the formation of the Presidential Commission on Critical Infrastructure Protection (PCCIP.)

The final report of this commission, released in November 1997, made several recommendations for future policy on information infrastructure protection. The commission calls for partnership between industry and government to share the responsibility. The report points out that the owners and operators of the commercial systems have the knowledge and access to defend their systems; while the government has the legal, regulatory, military and law enforcement resources to deter serious cyber threats. The Commission called for formation of a National Information Assurance Office to coordinate efforts to protect the NII.[7]

In 1996, the National Defense Panel studied the long-term issues facing national security. Among their conclusions they found that the key to defending the information infrastructure lies in the detection of an attack and the ability to quickly respond and recover from its effects. In dealing with cyber terrorism they state that the complexities of sharing intelligence and the hand off of responsibilities as the case transitions from DoD to the

State Department, to the Justice Department, is poorly delineated "and may, in some areas, be dysfunctional."[8] In supporting the findings of the PCCIP, the Panel affirmed that DoD "must play an active role in the process envisioned by the Commission and its roles should be made clear."[9] Critical to this role would be the sharing of information with law enforcement agencies.

The Panel put an even sharper focus on the defense of the NII from information warfare attacks by calling for formation of a new unified command, "Americas Command", responsible for defending the homeland.[10]

Our nation's warfighting forces depend on the NII for an uninterrupted flow of information to gain information superiority, and increase battlespace awareness in executing military actions as called for in the Joint Chiefs of Staff, Joint Vision 2010.[11] The NII has become a critical enabler to the success of military operations. Ninety-five percent of Department of Defense (DoD) information systems depend upon telecommunications provided by the commercial sector of the NII.[12] These commercial networks, regulated in part by federal, state, and local government; are significantly influenced by market forces.[13]

In March 1998, Secretary of Defense William Cohen gave information warfare, both defensive and offensive, more visibility and clout by establishing a new deputy assistant secretary for information operations within the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence

(ASDC3I). DoD has put resources behind its information defense efforts by funding them at $3.6 billion over five years.[14]

To ensure our dominance as a world power, our NII must be reliable, robust, secure and flexible to changing threats. It must be designed such that it degrades gracefully when attacked, still maintaining a minimum level of service. Catastrophic degradation of NII services could dramatically alter how we respond to a strategic threat. The social forces that would rise up from a nation used to the luxury of electronic commerce and "cruising the Net," may be more than our legislators could withstand. Unless our national leadership can assure people that they can continue to safely rely on information technology, public pressure may force national security policy changes that may not be in the nation's best interest.

WHAT IS THE NII?

To help understand the complexity of the NII, one can draw an analogy to the commercial transportation systems that move goods throughout our nation. Multiple types and sizes of railroads, highways, airlines, distribution centers, etc. interconnect to load and carry vehicles with various types of cargo. Each vehicle transits the network, just as independent packets of data transit telecommunications networks.

The transport systems operate together to get the right stuff to the right user. These transport networks do not have one central "brain", each portion manages itself. Yet remarkably the independent parts come together effectively to move the enterprise of our nation.

For example, you need a certain piece of unique hardware so you order it from a company. Since you wish your sensitive cargo protected, you ask for certain security measures such as locked containers, special handling, etc. The company packages the item, puts it in special packaging to protect it, then hands it over to a shipping company. The shipping company truck takes the item over city streets to a distribution center. At the center the package gets reloaded into a different, larger truck that carries it to your city via the interstate highway system. At your city the truck delivers the package to another distribution center, where it is transloaded to a smaller vehicle that uses the local roads to deliver it to your home.

Within this network the interstate style multilane highways and railroads serve as backbone transport paths. With their stations and on/off ramps serving as designated interface points to local road networks, and distribution centers serving as major redirection points, independent vehicles carry the cargo between local distribution facilities, stores, homes and other users.

Just as there are different categories of transportation means, the components of the NII fall into two basic categories, communications systems (roads, highways and distribution centers), and information applications (warehouses, stores, customers). Emerging technologies continue to blur the boundaries of these once very distinct areas.

- Internet
- Public Switched Telephone
- Data Networks
- Radio Networks
- Public Utilities Controls
- Cable TV
- Defense Command and Control Networks
- Television Networks
- Financial Networks
- Cellular Phone Networks
- Satellite Networks
- Fire and Police Communications
- On-line Services
- Broadcast Satellite TV

Table 1. Typical NII Networks

THREATS

Interconnectivity and widely dispersed automation throughout our critical infrastructures, with limited self-protection features, makes them susceptible and attractive targets. Innovative use of offensive cyber weapons against us make traditional notions of physical sanctuary less meaningful. Conventional military forces can do very little to protect us from cyber threats.

Our open society creates a target rich environment. Federal regulations require commercial activities to post information that is of great use to our adversaries. For example, the Department of Energy and the Environmental Protection Agency require government agencies and industry to post locations of nuclear material and hazardous waste to web pages on the internet in the interest of public awareness. Knowledge of the location of these materials also interests terrorists. Many government agencies use the Internet in the course of doing business. The Internet functions on the premise of technological information sharing. Each of the data hosts, routers and servers exchanges data on the hardware configurations, software configuration files and addresses of users. All of this information is a gold mine to an adversary seeking to disrupt our information networks.[15]

So far, most of the attacks on the NII have come from insiders,[16] but attacks from outsiders continue to increase in frequency.[17]

Information technology offers a would be cyber tamperer a high visibility, low-risk, cost-effective payoff.[18] It no longer requires expensive sophisticated equipment to pull signals out of the "ether" for exploitation. Now, with just a personal computer and modem, cyber adversaries can enter information systems to copy, disrupt, or destroy data when and where they please.

The "interstates" of our information systems are the high capacity communications systems such as microwave, fiber-optic and copper cable, and satellites. The biggest threat to these bulk carriers of data used to be that of adversarial intercept of the traffic on these systems.

Now, the greater threat comes from adversaries manipulating the automated systems and software that control and manage the backbone systems to deny or disrupt service. Countering this threat involves protecting these automated control systems.

The Defense Department's reliance on commercial systems combined with shrinking defense budgets will force procurements towards interoperability and common technical standards within DoD, other government agencies and the commercial sector. Reaching commonality of data format will promote a shared data environment with reusable, architecturally consistent components.[19]

However, it will be easier to adversely manipulate systems that use, and reuse, common protocols.[20] The great diversity of standards at present makes the job of technically exploiting more than any single standard complex and difficult. As we migrate to commonality, an adversary that gains the ability to exploit the standards suddenly can exploit the entire network.

Once an adversary gains access to a primary data router, he can manipulate where traffic flows. You can imagine the inconvenience it would cause you if an agent in one of the large freight distribution centers in Mechanicsburg, Pennsylvania, decided to start throwing your packages into a truck that never leaves the dock. You would never get your packages, but the system would think they were shipped.

Adversary access to these critical core controlling systems could result in an attack that causes a cascading effect on the entire system. A disruption at a key point could overload adjacent or connected systems, resulting in failures of other systems. What may seem a small isolated incident to one system manager may actually have serious cascading effects on other portions of the NII when seen from a broader perspective. Without the ability to see the broader view it would be difficult for national leaders and policy makers to determine who is responsible and what are their motivations behind seemingly isolated cyber incidents and make decisions on the proper response. As an example, the Federal

Computer Incident Response Capability (FedCIRC) states that of the 159 incidents they handled in First Quarter FY98, the incidents actually "rippled through tens of thousands of computer hosts and sites.[21]

CHALLENGES TO ACTION

Managing the consequences of an attack on the NII requires integration of capabilities and processes beyond the scope of any single military department, government agency, or commercial enterprise. The biggest problem we face is that we don't know what we don't know. The problems encountered are a whole new dimension than those we have experience in handling. No single entity either in government or the commercial sector controls more than a small portion of the whole. Although the NII sustains attacks on an increasingly frequent basis, each attack has its unique characteristics. With the lack of data sharing among stakeholders and the constantly changing face of the threat, there is limited empirical data to contribute to the study of the solution to our problems. There are many more questions than answers. It is hard to chart the path to meet your ends if you don't know where you are. It is also hard to design "sensors" to detect attacks, and estimate what damage they have caused, when you don't know what you are looking for.

Protecting the integrity of the network and reacting to system failures requires a great deal of human intervention today. System administrators and network managers must protect information systems against unauthorized access and against modification or denial of information.[22] An adversary who can co-opt a system administrator or enter a system at the administrator "superuser" access levels can strike the heart of a network. Access at this level opens doors to any of the files stored within the system.

Encryption programs and password regimes can protect key infrastructure components such as data routers and switches by preventing hackers and terrorists access to computer networks that control them.[23] Unfortunately, most commercial key infrastructure nodes are not protected well enough to prevent a dedicated adversary from gaining entry.

The information user wants assurance of the integrity of his information. To protect data elements during transmission across a network one must use a cryptographic device to "scramble" the signal so it cannot be interpreted by those who do not possess the key to the scrambling algorithm.

Congress is considering legislation which will free encryption technologies from export controls.[24] Allowing the rest of the world use of our commercial encryption technology will surely benefit commerce, but also increases vulnerabilities to exploitation of critical information protected by these encryption techniques. Proliferation of commercial encryption, with its attendant vulnerabilities, reinforces the necessity for using only approved, National Security Agency produced encryption for critical defense information.[25]

The ability to protect against transnational adversaries has recently become more complicated with the passage of the Telecommunications Act of 1996. This act opened up competition in the telecommunications industry, but also generated national security concerns as it allows foreign ownership of U.S. telecommunications companies.[26] It increases the difficulty of assuring the integrity of information systems when they are produced by international corporations with sub-units and employees in many nations who may not share the same political interests and compliance with regulations as US companies.

- Federal Government
- Military
- Industry
- Congress
- Public Interest Groups
- Politicians
- Academia
- International Economic Groups
- Local Government
- Regional Alliances

Table 2. Typical NII Stakeholders

The government can no longer afford to develop its own software except for some very unique niche applications. As a result, more and more commercial off the shelf software ends up in critical national defense systems. Corporate competition and profit drives companies to develop software packages as cheaply as possible. Many companies sub-contract writing of software code to off-shore, non-U.S. companies. It is too expensive to scan millions of lines of code to determine if these software writers inserted disruptive code into the program. The capability exists to wrap malevolent code in innocuous digital wrappers making it very difficult to determine if clandestine code exists in the software.

Just as the various highway departments, law enforcement agencies, corporate operations centers, and street department work together to keep our transportation network flowing, the "brains" provided by the various levels of communications management make all the divergent parts work together. The management layers establish and control system integrity and security.

It will take a cooperative effort of government and industry at the management layer of the information systems of the future. This government-civil interface is an enormously complex policy issue. As DoD increasingly relies on commercial vendors to perform management tasks, software development, electronic component maintenance and logistics, stronger partnerships must develop.

Sharing of information poses a dilemma for commercial enterprises. Their competitive advantage may depend on proprietary data they do not desire to share. In addition, sharing the details of a possible cyber attack may get out to the corporation's customers and result in loss of confidence in the company. The loss of client confidence could prove disastrous to corporations such as financial houses, stock brokers, and medical firms.

The balancing of the government necessity to access information with the right to individual privacy is a very difficult nut to crack. The Bill of Rights guarantees of certain rights to US citizens and residents, while restricting the authority of the federal government. The Fourth Amendment to the US Constitution guarantees citizens protection form unreasonable surveillance by the government. This makes it extremely difficult for the government to gather network data, because by its technical nature of who communicated with whom, for how long, etc., the data discloses much about the private lives of citizens. Even if the a government agency could collect this data, sharing it with others would have to address the stipulations of the Privacy Act of 1974, and the Paperwork Reduction Act of 1995, limiting the disclosure of information specific to any one individual. The Ninth Amendment states the principle that powers not specifically delegated to the Federal government are retained by the people.

It will be difficult for our legal system to clarify roles and responsibilities in an environment that increasingly moves away from traditional jurisdictional boundaries. Most legal authorities come from a time of geographical boundaries and physical limits to jurisdictions. They need a greater awareness of information security concerns in a "virtual world."[27] Jurisdiction in the case of a possible cyber attack becomes cumbersome. The virtual environment has no borders. An attack may appear to come from off-shore, when in reality it comes via electronic means from within. Many federal and state agencies could become involved, for example: Department of Justice, CIA, DoD, Treasury, and the FBI. Each would respond differently. Law enforcement activities would treat indicators of attack as evidence to be protected for its use in a trial, but national security agencies would want to respond using the data. The lack of codified international law further complicates the issue. Few countries have laws which address computer crime.[28]

Perhaps the greatest challenge in protecting the strategic capability of the NII is the ability to assess the nature and extent of damage from an attack in a timely manner, warn users and operators, decide upon a response, isolate and then repair the damage. The visibility of interdependent networks, in the aggregate, enabling managers to do battle damage assessments, does not currently reside in any one agency or corporation.

Managing consequences of attacks on anything the sheer size and complexity of the NII presents significant problems. Literally millions of communications links, fiber-optic cables, radios,, copper cables, switches, data routers, file servers, satellites, etc. interconnect to in a giant information cloud. Each one of these components generate telemetry data on each call, data packet or bit stream it processes. All of this telemetry must be analyzed to detect anomalies.

The Department of Defense has become fully engaged in the process of identifying threats, vulnerabilities and indications and warnings of information attacks on defense systems. Each of the military departments has established an agency to handle network intrusions.[29]

The problem with cyber threats is that the traditional sources of intelligence do not work. The speed of information attacks, combined with the shrouded identity of the attacker make it extremely difficult to detect attacks and especially who is attacking. Due to legal constraints, the intelligence community cannot collect on US persons and has therefore has difficulty monitoring and gaining access to sources of attack intelligence, (e.g. server logs, web browser activity logs, and system administration records).

Software to detect network intrusions has gained heightened federal attention with the publication of the PCCIP results. Intrusion detection software using artificial intelligence has the ability to collect massive amounts of data on information systems, recognize attack patterns, inform network management tools, and can be integrated with security firewalls. DARPA has funded several efforts to improve software in this area. Much needs to be done, particularly in the area of large-scale networks and elimination of false alarms according to Teresa Lunt, DARPA program manager, "Current detection software must work from an establish database on attack profiles. They cannot defend against a stealthy or unknown attack pattern."[30]

Each commercial service provider and each government agency that operates a portion of the NII has systems that monitor the general heath of their portion. Other systems track the users connected at each particular point and the priority of restoration for those users.

Although, individual hardware components have some built-in redundancy and diagnostic features, a central management facility must analyze the entire system for the effect of a failed component, then decide on actions to redirect other assets to provide the lost capability and/or direct appropriate repair or replacement actions. Human experts, when they detect an intrusion or a network anomaly, can take action. Unfortunately this takes time as they must sift through dozens of computer screens, pages of printout, etc. A cyber attack is a fleeting event. Taking too long to analyze and decide may mean strategic losses.

However, cooperation on sharing cyber attack information appears to be increasing. Attorney General Janet Reno recently announced the formation of a National Infrastructure Protection Center (NIPC). This center will provide near real-time "watch-and-warning" capabilities to help trace attacks back to the source. Initially, the NIPC will include representatives from the FBI, DoD, Transportation and Energy. Eventually, the center hopes to add representatives from the private sector.

The NIPC plans to use artificial intelligence software developed by DOE's Sandia National Laboratories and modeled on the Arms Control Treaty Monitoring System. This system will embed Intelligent Agent "sensors" in the computer systems of the nation's critical infrastructure to help detect attacks.[31]

RECOMMENDATIONS

The indicators of a cyber attack will manifest themselves technologically, but the solutions for our response will be found beyond technology in legal, political and sociological means. Current efforts to pull together government and commercial initiatives on infrastructure protection appear to be headed in the right direction. However, more work needs to be done on sharing data for managing consequences of cyber assaults in real-time. The best chance for successfully gaining the cooperation of the civil sector lies in Presidential action. The President should appoint a prominent citizen to head an Executive level agency charged with national information assurance as recommended by the PCCIP.

The risk assessments show that we cannot wait to react, we must proactively design our NII systems to absorb and react to malevolent disruptions. We must design systems that include alternate routing, component redundancy, imbedded security controls and automatic status reporting. These measures will require modest public and private investment, but not nearly equal to the expense of recovering from a relatively unsophisticated attack on unprotected vital components of the NII.

Technology such as artificial intelligence (AI) can help overcome the limitations of the human mind in dealing with magnitude of the challenge. The problems of managing consequences of a cyber attack on the NII are large, complex, time-sensitive and require human expertise. All of these characteristics fit the model for potential artificial intelligence applications to help meet the challenge.[32] Applications of artificial intelligence systems could improve real-time response to a cyber attack. AI systems could analyze the data and propose possible solutions to human decision makers. No one AI system could handle the complexity of this problem, however AI systems applied at several levels could dramatically help humans make decisions.

Use of AI applications to help manage consequences of cyber attack on the NII will require a greater understanding of AI by policy makers and corporate leaders. We can assist in broadening the national awareness of AI by fostering more AI education programs in service schools and universities. Also, the National Science Foundation should fund more research into this potentially beneficial technological discipline.

The current regulatory and legal frameworks make it cumbersome for government to influence information security, particularly in issues of transnational cyber attacks. Advances in technology outpace the ability of the law to adapt. Congress and the courts must develop law to clarify jurisdictions, and limits of liability in a "virtual" future that transcends historical institutional, international, and geographic boundaries. To entice corporations to pay more attention to information security, legislation should be introduced to hold corporations liable. Corporations who do not adhere to specific standards of resaonable protection should be held liable, not only for immediate damages and losses, but also for losses due to cascading effects.

We must keep protection of the NII a national security priority. Information comprises much of what we value and hold dear in America. The public having grown accustomed to the luxury of information technology will have little tolerance to loss of critical services.

CONCLUSIONS

The objective of a coordinated cyber attack upon the NII could be to gain strategic leverage over US decision makers. Therefore, our national leadership must take these attacks not only in the context of their immediate damage, but in terms of their influence upon public opinion.

The information age has brought enormous benefit to the United States. However, our reliance upon our information infrastructure has become a dependency resulting in strategic vulnerability to our military, economic and political power. Our national leadership recognizes how critical the NII is to national security and has taken steps to lead us toward assuring its viability.

The interdependency of civilian and military information networks makes it clear that ensuring the availability and security of critical defense information in the face of cyber assault will require a cooperative effort of government, military, and business. We are on the right track.

The ends, ways and means of managing the consequences of malevolent intrusion into the NII are within the capabilities of the nation to implement. There is no doubt we will suffer assaults on our information systems. Our success at dealing with these assaults, thus preventing an adversary from gaining strategic advantage and jeopardizing our way of life will hinge on taking action to resolve the technological, legal, and sociological impediments to information infrastructure protection.

"In information war, if an enemy's information or information systems are threatened to the point where national leadership must take action, then information warfare is underway."

John Alger
National Defense University

Word Count: 5667

ENDNOTES

[1] Report of the National Defense Panel, Transforming Defense: National Sec;urity in the 21st Century, (Arlington, VA: U.S. Government Printing Office, 1997), 27.

[2] The National Information Infrastructure (NII) includes the entire range of equiment and systems used to transmit, store, process and display voice, data, and images. It includes scanners, computers, telephones, switches, video and audio tapes, data routers, printers, microwave, satellite and optical fiber transmission lines, and much more. See also "What is the NII?" The National Information Infrastructure Agenda for Action, Available from <http//nii.nist.gov/nii>, Internet; accessed 16 December 1997.

[3] Jeffrey E. Garten, U.S. Undersecretary of Commerce for International Trade, "Trade and Foreign Policy: Reflections of Economic Diplomacy," Washington: U.S. Department of Commerce, July 1995.

[4] The White House, A National Security Strategy for a New Century (Washington, D.C.:U.S. Government Printing Office, 1997) 14.

[5] "About the President's Information Infrastructure Task Force," available from <http//www.iitf.nist.gov/>; Internet; accessed 17 December 1997.

[6] Office of the President of the United States, "EO 13010 Critical Infrastructure Protection 15 July 1996," available from <http://www.fas.org/irp/offdocs/eo13010.htm>; Internet; accessed 26 September 1997.

[7] "Critical Foundation, Protecting America's Infrastructure, The Report of the President's Commission on Critical Infrastructure Protection," October 1997; available from <http:www.pccip.gov/report_index.html>; Internet; accessed 13 November, 1997.

[8] Report of the National Defense Panel, Transforming Defense: National Sec;urity in the 21st Century, (Arlington, VA: U.S. Government Printing Office, 1997), 27.

[9] Ibid.

[10] Ibid, 72.

[11] The Joint Chiefs of Staff, Joint Vision 2010. (Washington, D.C.:Joint Chiefs of Staff, undated), 16.

[12] Kenneth A Miniham, "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal, 5, no.1 (Spring 1996):20.

[13] Office of the Secretary of Defense, Report of the Defense Science Board Task force on Information Warfare-Defense (IW-D), (Washington, D.C.:Department of Defense, 25 November 1996), Executive Summary.
Also available from <http://www.jya.com/iwd.htm>; Internet.

[14] Bob Brewin and Heather Harreld, "DOD adds attack capability to infowar," Federal Compuer Week, March 2, 1998:1,48.

[15] The ideas in this paragraph are based on remarks made by a speaker participating in the USAWC Information Warfare Issues class.

[16] Rutrell Yasin, "Security vendors Unveil Their Wares at N+1," Internet Week, 20 October 1997.

[17] Some examples of recent cyber attacks:

March, 1998. Hackers attack US Air Force and Navy systems in a game of hacker "King of the Hill.'

March, 1997. A computer cracker for Sweden penetrated the 911 emergency sysems of North Florida, tying up the lines for asignificant period of time.

1997. The World Lynx Corporation, an Arkansas-based Internet service provider had its server attacked by a hacker who interrupted service for an entire day.

February, 1997. Three teenage hackers from Croatia broke into the Pentagon's computers and allegedly stole classified files. Damage estimated at one-hal milliondollars.

February, 1997. Unknown hackers replaced the U.S. Air Force homepage on the WWW.

For a more comprehensive unclassified listing of cyber attacks see: <http://www.georgetown.edu/users/samplem/iw/html/database.html>; Internet; accessed 16 December, 1997.

See also statistical and trends reports of the Federal Computer Incident Response Center available at <http//fedcirc.llnl.gov/>; Internet, accessed 14 March, 1998.

[18] Mattehw G.Devost, Brian K. Houghton and Neal Apollard, "Information Terrorism: Can you Trust Your Toaster?" available from <http://www.terrorism.com/terrorism/itpaper.html>; Internet; accessed 16 December 1997. *Note: A longer version of this paper was first place winner of the National Defense University's Sun Tzu Art of War Research Award in Information Warfare.*

[19] Dawn Hartley, "Shared Data Environment," briefing, AFCEA Conference, 17 December, 1997, available from

<http:spider.osfl.disa.mil/dii/brief/AFCEA_brief/afcea_brief.html>, Internet; accessed 22 January 1998.

[20] Robert K. Ackerman, "Digital Formats Complicate Information Security Tasks," Signal Vol 51. No.6 (February 1997): 22.

[21] FedCIRC "Statistics and Trends Report 1st Quarter FY 98." Available from <http://fedcirc.llnl.gov/articles/incidents0298.html> Internet; accessed 14 March 1998.

[22] Joint Chiefs of Staff, Defensive Information Operations Implementation, CJCSI 6510.01B (Washington D.C.: Department of Defense, 22 August 1997), GL-11.

[23] Asron Pressman, "U.S. cyberterrorism report hit on encryption stance," Reuters, 5 November, 1997. Available from <http:www.infowar.com/civil_de/civil_de110797a.html-ssi> Internet; accessed 29 November 1997.

[24] John Rendleman, "Backdoor Closes, For Now, On Crypto Plan," Internet Week, 29 September, 1997.

[25] "Welcome to MISSI," available from <http:www.nsa.gov:8080/programs/missi/index/html>; Internet; accessed 30 January 1998.

[26] The Joint Staff, Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd ed. (Washington D.C.:The Joint Staff, 4 July 1996),2-38.

[27] "Critical Foundation, Protecting America's Infrastructure, The Report of the President's Commission on Critical Infrastructure Protection," October 1997; available from <http:www.pccip.gov/report_index.html>; internet; accessed 13 November, 1997.

[28] The Joint Staff, Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd ed. (Washington D.C.:The Joint Staff, 4 July 1996),2-43,45.

[29] For a detailed listing of organizations and agencies dedicated to computer incident response see <http://www.securezone.com> and <http://www.cert.org> internet; accessed 14 March 1998.

[30] John Moore, "Novell, detection gear share spotlight," Federal Computer Week, October 20, 1997, 48.

[31] Heather Harreld and Torsten Busse, "Cybercenter will trace net intrusions,". Federal Computer Week, March 2, 1998, 1,48.

[32] United States Military Academy, Artificial Intelligence-An Executive Overview (West Point: United States Military Academy, 1994), 10.

BIBLIOGRAPHY

Ackerman, Robert K. "Digital Formats Complicate Information Security Tasks," Signal, Vol. 51. No. 6 (February 1997), 22.

Braunberg, Andrew C. "Brain's Affinity for Imagery eases Information Overload," Signal, Vol. 51, No. 4 (December 1996), 49.

Brewin, Bob. "DoD unveils flexible messaging architecture," Federal Computer Week, December 1, 1997, 46.

Brewin, Bob and Heather Harreld. "DOD adds attack capability to infowar." Federal Computer Week, March 2, 1998, 1,48.

"Critical Foundation, Protecting America's Infrastructure, The Report of the President's Commission on Critical Infrastructure Protection." October 1997. Available from <http:www.pccip.gov/report_index.html>. Internet. Accessed 13 November, 1997.

DeVost, Matthew G., Houghton, Brian K. and Apollard, Neal. "Information Terrorism: Can you Trust Your Toaster?" Available from <http://www.terrorism.com/terrorism/itpaper.html> Internet. Accessed 16 December 1997. *Note: A longer version of this paper was first place winner of the National Defense University's Sun Tzu Art of War Research Award in Information Warfare.*

FedCIRC, "Statistics and Trends Report, 1st Quarter FY 98." Available from <http://fedcirc.llnl.gov/articles/incidents0298.html> Internet. accessed 14 March 1998.

Garten, Jeffrey E. U.S. Undersecretary of Commerce for International Trade. "Trade and Foreign Policy: Reflections of Economic Diplomacy." Washington: U.S. Department of Commerce, July 1995.

Grier, Peter. "At War With sweepers, Sniffers, Trapdoors and Worms." Air Force Magazine, March 1997, 20-24.

"Hacker Threats to Defense Computer Systems." Available from Newsbytes News Network: <http://www.newsbytes.com/DODHACK/>. Internet. Accessed 16 December, 1997.

Harreld, Heather. "Security team in money crunch," Federal Computer Week, December 1, 1997:14.

________. "FBI, companies join forces to guard against cyberattacks." Federal Computer Week, December 15, 1997, 1.

Harreld, Heather and Torsten Busse, "Cybercenter will trace net intrusions." Federal Computer Week, March 2, 1998, 1,48.

Hartley, Dawn "Shared Data Environment." Briefing. AFCEA Conference, 17 December, 1997. Available from <http:spider.osfl.disa.mil/dii/brief/AFCEA_brief/afcea_brief.html>. Internet. Accessed 22 January 1998.

"IW Study May Guide U.S. Policy," Defense News, March 10, 1996.

Joint Chiefs of Staff. Approved Terminology. Joint Pub 1-02, DoD Dictionary. Washington D.C.: Department of Defense. April 1997.

________. Defensive Information Operations Implementation. CJCSI 6510.01B. Washington D.C.: Department of Defense, 22 August 1997.

________. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. 2d ed. Washington, D.C.:Joint Chiefs of Staff, 4 July 1996.

________. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1 Washington: Department of Defense. 7 February 1996.

________. Joint Vision 2010. Washington, D.C.:Joint Chiefs of Staff, undated.

________. "Shape, Respond, Prepare Now, A Military Strategy for a New Era." Available from <http://www.dtic.mil/jcs/nms/>. Internet. Accessed 6 October 1997.

Libicki, Martin C. Defending Cyberspace and Other Metaphors. Washington, D.C.:National Defense University, 1997.

________. "What is Information Warfare. Available from <http://www.ndu.edu/ndu/inss/strforum/forum28.html>. Internet. Accessed 17 September 1997.

Miniham, Kenneth A. "Intelligence and Information Systems Security: Partners in Defensive Information Warfare." Defense Intelligence Journal. 5, No. 1 (Spring 1996).

Moore, John. "Novell, detection gear share spotlight," Federal Computer Week. October 20, 1997.

Office of the President of the United States. "EO 13010 Critical Infrastructure Protection 15 July 1996." Available from <http://www.fas.org/irp/offdocs/eo13010.htm>. Internet. Accessed 26 September 1997.

Office of the Secretary of Defense. Report of the Defense Science Board Task force on Information Warfare-Defense (IW-D). (Washington, D.C.:Department of Defense, 25 November 1996).

Peters, Ralph. "Constant Conflict," Parameters (Summer 1997): 4-14.

________. "The Culture of Future Conflict," Parameters (Winter 1995-96).

Pressman, Asron. "U.S. cyberterrorism report hit on encryption stance." Reuters, 5 November, 1997. Available from <http:www.infowar.com/civil_de/civil_de110797a.html-ssi> Internet. Accessed 29 November 1997.

Rendleman, John. "Backdoor Closes, For Now, On Crypto Plan," Internet Week, 29 September, 1997.

Report of the National Defense Panel. Transforming Defense: National Security in the 21st Century. Arlington, VA: U.S. Government Printing Office, 1997.

Schwartau, Winn. "Information Warrior." interview by Ben Venzke. Wired. August 1996, 137.

Selden Zachary. "Information Security: The implications of Cyberwar for National Security and Business." Available from <http://www.infowar.com/civil_de/civil_102097a.html-ssi>. Internet. Accessed 20 November 1997.

Staten, Clark. "Report: Emergency Response and Research Institute." Available from <http://www.infowar.com.civil_de/civil_103097b.html-ssi> Internet. Accessed 29 November 1997.

Toffler, Alvin, and Heidi Toffler. War and Anti-war: Survival at the Edge of the 21st Century. New York: Bantam Books, 1990. 585pp.

The National Security Telecommunications and Information Systems Security Committee (NSTISSC). Available from <http://www.dtic.mil:80/c3i/ntissc.html>. Internet. Accessed 14 October 1997.

The White House. A National Security Strategy for a New Century. Washington, D.C.:U.S. Government Printing Office, 1997.

"The National Security Telecommunications and Information Systems Security Committee (NSTISSC)." Available from <http://www.dtic.mil:80/c3i/ntissc.html>. Internet. Accessed 14 October 1997.

United States, National Communications system, The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document (Arlington, VA.: National Communications System, 1994), 2-24.

U.S. Department of Defense. Information Operations. Directive TS-3600.1. Washington, D.C.:U.S. Department of Defense, 9 December 1996.

________. Information Warfare A Strategy for Peace...The Decisive Edge in War. undated.

________. Report of the Quadrennial Defense Review. Washington, D.C.:U.S. Department of Defense, May 1997.

United States Military Academy. Artificial Intelligence-An Executive Overview. West Point: United States Military Academy, 1994.

Washington, Douglas. "Onward Cyber Soldiers," TIME, 21 August 1995.

"Welcome to MISSI." Available from <http:www.nsa.gov:8080/programs/missi/index/html>. Internet. Accessed 30 January 1998.

"What is the NII?" The National Information Infrastructure Agenda for Action. Available from <http//nii.nist.gov/nii>, Internet. Accessed 16 December 1997.

Yasin Rutrell. "Security vendors Unveil Their Wares at N+1," Internet Week, 20 October 1997.